REMARKS

These remarks are in response to the Final Office Action dated September 17, 2008 (Office Action). As this reply is timely filed, no fee is believed due. In consequence of this Amendment, claims 1, 12, and 20 have been amended and claims 4 and 17 have been cancelled. Claim 21 was cancelled by prior amendment. Accordingly, claims 1-3, 5-16, 18-20, and 22 remain pending.

Rejections Under 35 U.S.C. § 103(a)

Claims 1-18, 20, and 22

Claims 1-18, 20, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,981,153 to Pang et al. (Pang) in view of U.S. Patent No. 6,496,971 to Lesea et al. (Lesea).

Claim 1 has been amended to recite the features previously recited in claim 4. As such, claim 1 recites "wherein the decryptor is a software decryptor stored in a memory and executed by the microcontroller, wherein the system further comprises hardware that selectively enables access to the key storage register by allowing the microcontroller access when a program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory."

The Office Action contends that Pang discloses a decryptor that is a software decryptor stored in a memory and executed by the microcontroller at column 13, lines 37-56. The cited portion of Pang discloses a method of operation for a decryptor where multiple keys may be used to encrypt data. Nowhere within the cited passage, however, does Pang state that the method is implemented within software, e.g., executing within a microcontroller. The Office Action has already conceded that "Pang does not explicitly disclose a microcontroller within the PLD for receiving an encrypted bitstream." It is this microcontroller, which the Office Action concedes is missing from Pang, that executes the decryptor.

The Office Action further contends that "hardware that selectively enables access to the key storage register by allowing the microcontroller access when a

program counter of the microcontroller specifies an address within an address range corresponding to the software decryptor within the memory" is taught by both Lesea and Pang. In particular, the Office Action cites column 6, lines 40-53 of Lesea and column 20, lines 27-53 and FIG. 16 of Pang.

Claim 1, as amended, states that access to the key storage register, which stores key data, is selectively permitted based upon an address of the program counter being within an address range in memory that corresponds to the address range in which the decryptor is stored. As known, the program counter is a specific register within the microcontroller itself. Depending upon the implementation of the microcontroller, the program counter stores the address of the current software instruction being executed by the microcontroller or the address of the next instruction to be executed by the microcontroller. Because the decryptor is implemented in software, one can determine that the decryptor is active, e.g., executing, within the microcontroller, when the address specified by the program counter is within the range of addresses in memory that correspond to the decryptor. In this manner, access to the key storage register depends upon the address of the instruction being executed or about to be executed by the microcontroller.

Column 20, lines 27-53 of Pang are wholly unrelated to selectively enabling access to a key storage register based upon the address of the program counter of a microcontroller. The cited passage relates to FIG. 16, which describes a process for performing readback, e.g., reading back information from configuration memory. The passage describes how configuration logic accesses the configuration memory for performing readback using the address decoder. An address of configuration memory from which data may be read is unrelated to the address stored in the program counter which specifies a current or next instruction to be executed. Nothing in the cited passage describes a decryptor executing within a microcontroller. Moreover, nothing in the cited passage relates to the use of an address of a program counter of a microcontroller. The passage simply describes the way in which configuration memory of a field programmable gate array is accessed or addressed.

Similarly, column 6, lines 40-53 of Lesea describe the process of reading from, or writing to, a configuration memory cell. This is the electrical process of bringing

particular address lines, e.g., wires, high or low to store a bit within configuration memory or to read a bit from configuration memory. The Office Action quotes a paragraph taken from column 6, lines 40-53 of Lesea within the "Response to Arguments" in support of the rejection of claim 4.

This passage, like the passage cited in Pang, is wholly unrelated to using an address within the program counter of a microcontroller to selectively provide access to a key storage register. As noted, the particular address of configuration memory that is the subject of a read/write operation is unrelated to the address of the instruction that is being executed or that will be executed. Nowhere within the cited passage is a program counter discussed or mentioned. Indeed, a text search of the entirety of Lesea for the phrase "program counter" yielded no results.

In further support of the notion that Lesea does not recite the elements of amended claim 1, claim 1 explicitly states that the decryptor is implemented within software. By comparison, in column 8, lines 21-23, Lesea states that "[w]hereas X register 115, Y register 113, decoders 114 and 116, frame buffer (frame register) 110, and readback buffer 112 of FIG. 3 are realized using dedicated hardwired logic...." Even presuming that decoders are the same as decryptors, which Applicants do not concede is the case, Lesea states that such structures are hardware. This means that using a program counter to determine when the software decryptor is executing and may access the key storage register is not taught or even suggested by Lesea.

In sum, both Pang and Lesea describe reading from and/or writing to particular configuration memory addresses. Neither reference discusses a program counter of a microcontroller or conditions access to the key storage register by the microcontroller based upon the address stored within the program counter as recited in claim 1.

Independent claims 9, 12, 18, and 20 include one or more features similar to those discussed within these remarks and are believed to be allowable for the same or similar reasoning. The remaining claims rejected under the combination of Pang and Lesea are believed to be allowable by virtue of their own merits and their dependence upon the underlying independent claims.

Since the combination of Pang and Lesea does not render Applicants' claims obvious, withdrawal of the 35 U.S.C. § 103(a) rejection of claims 1-3, 5-16, 18, 20, and 22 is respectfully requested.

Claim 19

Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Pang and Lesea in view of U.S. Patent No. 5,409,661 to Kuranaga. Applicant continues to proceed with the understanding that the citation of U.S. Patent No. 5,409,661 was a typographical error and that U.S. Patent No. 5,408,661 to Kuranaga (Kuranaga) was the intended citation.

Kuranaga discloses a memory controller that determines whether a next instruction to be executed exists within an internal random access memory (RAM) or an external read only memory (ROM). If the program counter value is within the range of addresses that exists within RAM, the controller retrieves the desired instruction from the internal RAM. Otherwise, the controller retrieves the instruction from the external ROM. This is analogous to a conventional memory controller that must convert virtual addresses to physical address and control the loading of pages into physical RAM. This procedure is unrelated to decrypting a bitstream using a microcontroller and controlling access to the key storage register by the microcontroller via the program counter.

Kuranaga fails to address the deficiencies of both Pang and Lesea in that, again, nothing in Kuranaga restricts access to a key storage register that stores key data based upon a program counter. Moreover, Kuranaga looks at the entire range of addresses stored within RAM rather than determining whether the address being executed indicates that a particular program, e.g., the decryptor, is being executed. Only when that program is executed is the microcontroller able to access the key storage register. Kuranaga merely determines the location of the next instruction to be executed and retrieves that instruction.

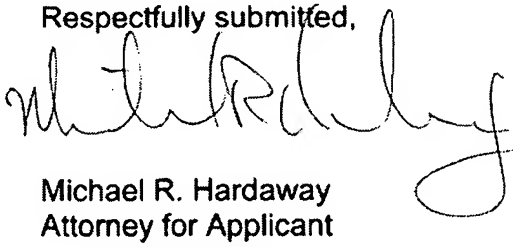
As neither Pang, Lesea, Kuranaga, nor any combination thereof renders claim 19 obvious, withdrawal of the 35 U.S.C. § 103(a) rejection of claim 19 is respectfully requested.

CONCLUSION

Claims 1, 12, and 20 have been amended herein. Claims 4, 17, and 21 have been cancelled. All claims are now in condition for allowance and a Notice of Allowance is respectfully requested.

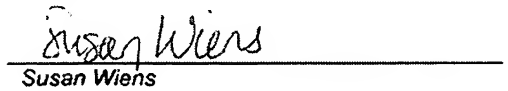
If there are any questions, the Applicants' attorney can be reached at Tel: 408-879-6149.

Respectfully submitted,



Michael R. Hardaway
Attorney for Applicant
Reg. No. 52,992

I hereby certify that this correspondence is being filed via EFS-Web with the United States Patent and Trademark Office on November 12, 2008.



Susan Wiens